

Общий регламент по защите данных (GDPR) может привести к возникновению ряда проблем в связи с блокчейном

Общий регламент по защите данных (GDPR), принятый Европейским союзом 25 мая 2018 года, в данный момент является наиболее обсуждаемым законодательным актом в Европе. В нем содержатся максимально строгие требования в отношении сбора и обработки личных данных, что может оказать существенное влияние на применение новых технологий. Например, блокчейн является одной из самых «горячих» тем в современном технологическом мире, однако в своем нынешнем виде он, по всей вероятности, не соответствует требованиям GDPR.

Какие данные можно классифицировать в качестве личных данных в рамках блокчейна?

Согласно GDPR, личные данные – это данные, связанные с идентифицированным или подлежащим идентификации физическим лицом. Псевдонимизированные данные классифицируются в качестве личных данных, и только лишь анонимные данные выходят за юридические рамки, установленные GDPR. Таким образом, в рамках блокчейна личными данными можно считать два типа данных: общедоступные ключи и данные о сделках, которые хранятся в блоках. Данные о сделках и общедоступные ключи являются псевдонимизированными данными. Хотя общедоступные ключи – это всего лишь ряд цифр, все же возможно при помощи дополнительной информации, например IP-адреса, установить личность. Данные о сделках являются зашифрованными или хешированными данными, так что можно считать, что речь идет об анонимных данных. И все же зашифрованные данные можно расшифровать при помощи подходящих ключей, и по этой причине они не являются необратимыми, как того требует GDPR от анонимных данных. Рабочая группа по защите данных, учрежденная на основании статьи 29, дает определение процессу хеширования как технике псевдонимизации, таким образом, функция хеширования не помогает решить проблему.

Кто является контролером данных в рамках блокчейна, или кому адресованы обязательства, перечисленные в GDPR?

Блокчейн – это рассеянная база данных, которой могут пользоваться все пользователи без централизованного контроля. С одной стороны, ни один из пользователей не является настолько же квалифицированным, как и контролер данных, однако любой пользователь может быть контролером. Самого субъекта данных также можно считать контролером данных, т.к. субъект данных имеет приватный ключ, и именно он является тем человеком, который в личных целях добавляет личные данные в блокчейн. Таким образом, в зависимости от действий, выполняемых в блокчейне, и от типа блокчейна, контролер данных или их обработчик может в каждом конкретном случае различаться.

В какой сфере применяются обязательства, установленные в GDPR?

GDPR применяется в отношении контролеров или обработчиков данных, действующих в Европейском союзе, или которые выполняют действия по обработке данных, связанные с предложением товаров и услуг субъектам данных в Европейском союзе или с наблюдением за поведением субъектов данных. Поскольку майнеры находятся по всему миру, и хешированием данных, которые находятся в блокчейне, занимается случайно выбранный майнер, на основании GDPR любого майнера можно считать обязанным лицом.

Обеспечение прав субъектов данных в блокчейне

GDPR устанавливает новые права, такие как, например, право на забвение и право на внесение изменений в личные данные. Эти права, по всей вероятности, станут наиболее серьезными проблемами в рамках блокчейнов. Блокчейн – это неизменная технология. Это означает, что все сохраняемые данные являются общедоступными и не подлежат изменению или удалению. Тот факт, что данные не подлежат удалению, является одной из важнейших ценностей блокчейна, а также наиболее серьезной проблемой, т.к. согласно GDPR, субъект данных должен иметь возможность потребовать от обработчика данных удаления личных данных.



KATRIN SARAP

VANDEADVOKAAT, PARTNER

(+372) 66 76 440

KATRIN.SARAP@NJORDLAW.EE